REMARKS

Claims 1-12 are pending in the application and stand rejected.

Rejection under 35 U.S.C §112

Claims 1, 5, 9, 11 and 12 stand rejected under 35 U.S.C. 112 as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention. In particular, the Examiner finds that the narrative nature of these claims renders them uncertain. Applicant has amended the claims to address the Examiner's perceived deficiencies and respectfully submit that the amendments as amended herein are clear and unambiguous. These amendments are made solely for the purpose of clarifying the scope of the claims and Applicant expressly notes that therefore these amendments are not made for purposes related to patentability because they do not alter the scope of the claims but rather merely clarify it.

Rejection under 35 U.S.C §103

Claims 1-12 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 6,134,550 to Oorschot et al. in view of The Book of Applied Cryptography by Menezes et al. In particular, the Examiner finds that Oorschot discloses all claimed steps with the exception of seeking a backwards proof, and that Menezes teaches precisely the seeking of a backwards proof of a primary goal by set out in Applicant's claim 1. The Examiner thus opines that it would have been obvious to one of ordinary skill in the art to utilize Menezes' method of using backtracking proofs because doing so offers the advantage of removing the need for a central trusted authority.

Applicant has reviewed the two references with care, paying particular attention to the passages cited to by the Examiner, and is compelled to disagree with the Examiner's understanding of these references. Claim 1 includes the limitation of "seeking a backwards proof of said primary goal by a process of recursively taking a goal to be proved, starting with said primary goal, and decomposing it into subgoals one of which corresponds to an attribute delegation that is justified by an available certificate and has the same subject as the goal being

decomposed, inability to decompose a subgoal that has not been proved causing the process to backtrack to a previous subgoal to seek a new decomposition of the latter." There is absolutely no disclosure in Menezes of the concept of decomposing a primary goal into subgoals to seek a proof. The concept discussed by Menezes is that of providing certificate paths between certification authorities in a strict hierarchy wherein a CA lower in the hierarchy can create certificates certifying the public keys of its directly superior CA – a so-called hierarchy with reverse certificates. Creating a reverse certificate is not the same as seeking a proof by recursively decomposing a primary goal into subgoals until able to produce a chain of subgoals proved by corresponding certificates that grounds in a subgoal justified by a justified attribute delegation that has as issuer the said known trusted issuer included in said primary goal. A simple way of assessing the utter lack of common ground between the two concepts is attempting to apply the claimed concept of seeking a backwards proof to the professed goal of Menezes in the context of Menezes' figure 13.9(d). As the Examiner will appreciate, seeking a backwards proof as per claim 1 will not, and indeed cannot, provide alternative routes to the root CA. Applicant therefore submits that claim 1 is allowable and respectfully requests the Examiner to reconsider and pass the claim to issue.

Claims 2-12 depend from claim 1. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Therefore, in light of the above discussion of claim 1, Applicant submits that claims 2-12 are also allowable.

Regarding the prior art made of record by the Examiner but not relied upon, Applicants believe that this art does not render the pending claims unpatentable.

Applicant further submits new claims 13-36, directed to a system and a computer program product that parallel original claims 1-12 as amended herein. A check for the excess claims fee is included herewith.

In view of the above, Applicant submits that the application is now in condition for allowance and respectfully urges the Examiner to pass this case to issue.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 12-0415. In particular, if this response is not timely